



**The right item, right place,
right time.**

Privacy Act 102 Privacy Training for DLA Supervisors / Managers



Privacy Refresher

From **Privacy Act 101**, you know that the Privacy Act is ...

- A statute that applies to the Executive Branch of the Federal government.
- Applies to U.S. citizens & lawfully admitted aliens
- “. . . a means to regulate the collection, use, and safeguarding of personal information.”





Privacy Refresher (cont'd)

In **Privacy Act 101**, you also learned that the Privacy Act:

- Covers “systems of records” – A group of records that
 - Contains a personal identifier (name, SSN, badge #, etc.);
 - Contains one other element of personal data; and
 - IS retrieved by personal identifier
- Provides U.S. Citizens/Lawfully Admitted Aliens with Guaranteed Rights –
 - To access/amend their records
 - To appeal agency decisions
 - To sue for breaches





Privacy Refresher (cont'd)

Privacy Act 101 also taught you that:

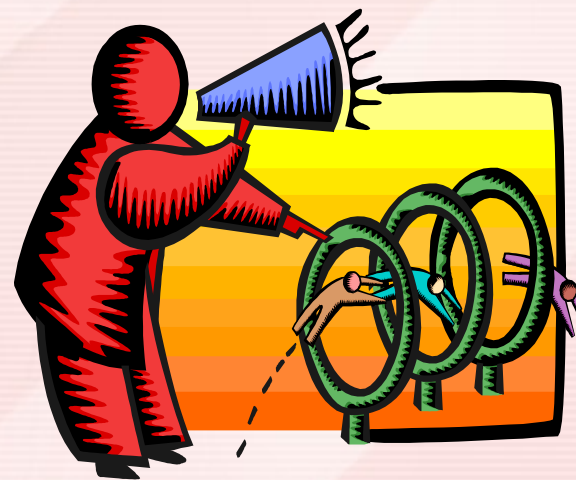
- Agencies may not collect data without first publishing a system notice in the Federal Register announcing the collection.
- The system of records notice sets the rules for collecting, using, sharing, and safeguarding data.
- The DLA and Government-Wide Privacy Act system notices are at <http://www.dod.mil/privacy>.





Do you Supervise Employees, Military Members, or Contractors Who . . .

- Initiate data collections?
- Receive Privacy data in the course of conducting DLA business?
- Create, manage, or oversee files or databases containing personal data?
- Disseminate personal data?





If “Yes,” You Have a Duty to Ensure that . . .

- Your staff receives Privacy Act training.
- No data collection is undertaken unless DLA has published a system notice covering the collection.
- Access to data is limited to those employees specifically assigned to the program - not all office employees!
- Data is transmitted in a secure manner.
- Data is safeguarded during and after duty hours.
- Your staff is complying with the Privacy Act, the DoD Privacy Program (32 CFR part 310), the DLA Privacy Program (32 CFR part 323), and the DLA Code of Fair Information Principles.
- Your staff is following DLA Information Assurance guidelines.





Supervisor's Roadmap For Meeting Privacy Responsibilities

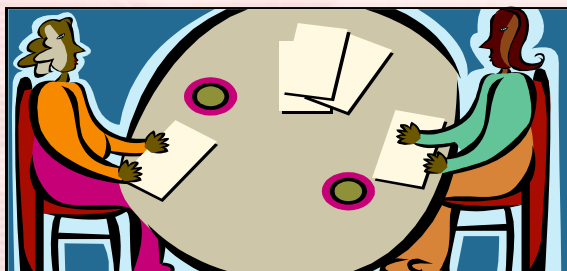
- Is Your Staff Privacy-Trained?
 - Ensure your staff annually reviews **Privacy Act 101** training, available at http://www.dla.mil/public_info/efoia
- Are Your Data Collections Properly Conducted?
 - Ensure your staff consults with your local DLA Privacy Officer before –
 - Initiating new data collections.
 - Adding new elements to an existing, approved database.
 - Creating or revising forms that collect personal data.
 - Deploying surveys.
 - Ensure your staff includes a Privacy Act Statement on all forms, surveys, or websites that collect personal data to be maintained in a system of records.





Supervisor's Roadmap For Meeting Privacy Responsibilities (cont'd)

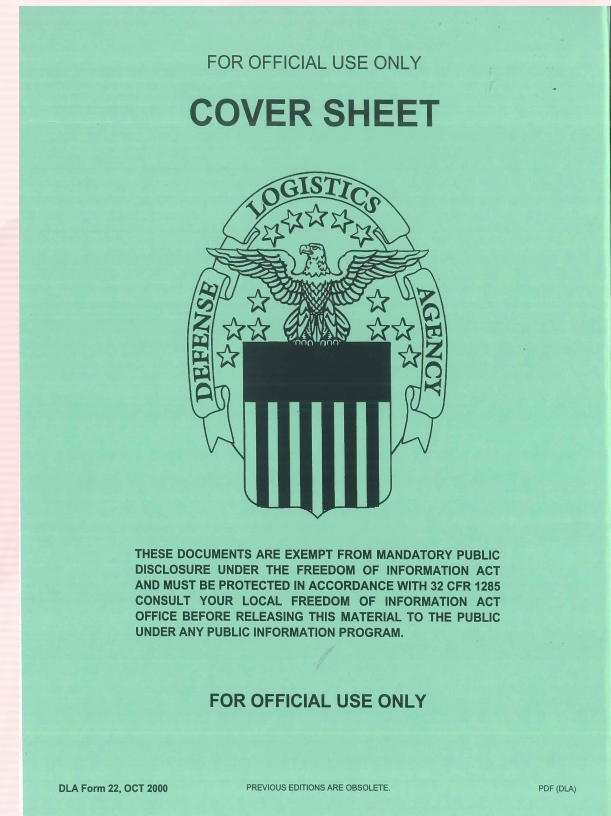
- Do You and Your Staff Practice Limited Access Principles?
 - Grant access to only those specific employees who require the record to perform specific, assigned duties.
 - Your staff must closely question other DLA individuals who ask for your data.
 - Why do they need it? How will it be used?
 - Is the purpose compatible with the original purpose of the collection?





Supervisor's Roadmap For Meeting Privacy Responsibilities (cont'd)

- Are Your Workers Transmitting Personal Data Properly?
- Do not use “holey joes” or interoffice mail envelopes to route personal data. Use sealable, opaque envelopes addressed to an authorized recipient.
- When hand carrying, use DLA Form 22 (FOUO Cover Sheet).
- When E-mailing personal data –
 - Use Common Access Card protocols to ensure confidentiality.
 - Verify that **each** addressee is an authorized data recipient.





Supervisor's Roadmap For Meeting Privacy Responsibilities (cont'd)

- Is Your Staff Safeguarding Personal Data?
 - Mark records “For Official Use Only” when created.
 - For electronic records, include “For Official Use Only” on data screens and in headers/footers of printouts.
 - Place records in file cabinets, overhead bins, or desk drawers for overnight storage.
 - Cover paper records when a third party enters the workspace.
 - Use filter screens on terminals to blacken angular views.



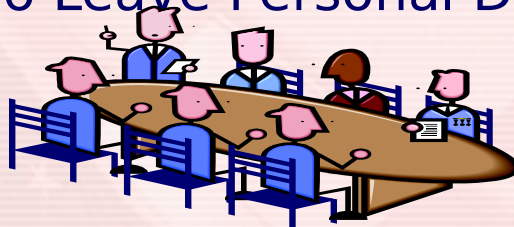
Supervisor's Roadmap For Meeting Privacy Responsibilities (cont'd)

- Is Your Staff Following the DLA Code of Fair Information Principles?
 - Periodically ask your staff to review the DLA Code of Fair Information Principles in the Privacy Act 101 training module. (Also included at slides 22-25 of this training module.)
- Is Your Staff Following DLA Information Assurance Guidelines?
 - Lock terminals when leaving the work area for brief periods.
 - Immediately report to you, your local Privacy Act Officer, or the Information Technology staff instances of personal data posted to public or shared websites, E-workplace, shared calendars, or shared drives.



Keeping Privacy at Top of Mind

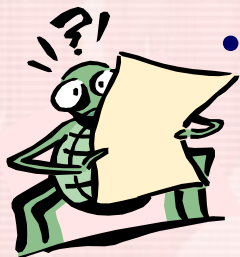
- Use Staff Meetings to Stress Good Privacy Practices.
 - Voice your commitment to protecting individual privacy.
 - Applaud workers who practice good privacy principles!
 - Remind staff to use caution when posting data to shared drives, e-workplace, or multi-access calendars.
 - Post no personal data.
 - Periodically review shared devices for compliance.
- Question Workers Who Leave Personal Data in the Open.





Keeping Privacy at Top of Mind (cont'd)

- Question Employees Who Fail to Lock Terminals When Leaving the Work Area.
- Scrutinize Proposed New Data Collections and Surveys.
 - Ask project managers to consult with the Privacy Act Office.
- Contracting out a Function?
 - Include the Federal Acquisition Regulation Privacy clauses in the contract (FAR 52-224-1 & 52.224-2).
 - Include language in the contract addressing how the data is to be disposed of at contract end.
 - Contact the Privacy Office for more requirements.





Supervising Privacy Act System Managers

- A “System Manager” is an individual assigned to oversee, manage, direct, and control a Privacy Act system of records. System managers require specialized Privacy Act training.
- System Manager Duties:
 - Comply with 32 CFR part 310 and part 323.
 - Follow Rules in the published System of Records Notice.
 - Respond to First-Party Access and Amendment Requests.
 - Determine if Third-Party Disclosures are Authorized.
 - Maintain an Accounting of all Third-Party Disclosures.
 - And More!
- System Managers may not institute changes to a system without first consulting with the DLA Privacy Act Office. Encourage your System Managers to work closely with the DLA Privacy Act Office in executing their duties.



Discussing Privacy Matters

- When discussing a person's health, financial affairs, personnel actions, criminal history, family affairs, or other personal aspect of his or her life, it is important to remember that details should not be brought up in staff meetings or discussed in common areas
- Personal matters should never be discussed with anyone without a strict need to know.





Examples of Personal Data?

PERSONAL DATA

- Electronic & physical home address and phone number
- Type of leave used (not admin or holiday)
- Performance rating
- Health, financial, & medical data
- Misconduct information
- On the job injury data
- Gov't-paid, personal development training, e.g. -
 - "Rid Yourself of Debt"
 - "Coping with your Unruly Child"
 - "Beating your Drug Habit"

NON-PERSONAL DATA

- Position description & duties
- Job title, series, and grade
- Duty address (but not overseas)
- Duty schedule (days & hours)
- The fact that an employee is on leave, teleworking, at an official function, not present for duty, or on a CDO.
- Gov't paid, work-related training, e.g. -
 - "Providing Good Customer Service"
 - "Become a Great Public Speaker"
 - "Principles of Grammar"



Alert Recall Rosters



- Employees are required to give supervisors their home telephone numbers, but they do not have to agree to share them with co-workers.
- If an employee objects to having his/her telephone number placed on a recall roster:
 - List “Unlisted” or “Unpublished” instead of home number.
 - Arrange to call the employee yourself during alerts or exercises.
- Remember to mark the recall roster “For Official Use Only.”
- Instruct your staff that the roster is to be used for official purposes only and kept in a secure location.



When Data Maintained By DLA or DLA Contractors Is Lost, Stolen, Or Compromised . . .

- Notify affected individual(s) within 10 days.
- Coordinate notification with the Privacy Act Office.
- Covered Individuals:
 - Military members and retirees.
 - Civilian employees (appropriated or non-appropriated).
 - Family members of a covered individual.
 - Other individuals affiliated with DoD (e.g., volunteers).
- As a minimum, advise individual of:
 - Data elements involved.
 - Circumstances surrounding the incident.
 - What protective actions the individual can take.





Lost, Stolen, or Compromised Data (cont'd)

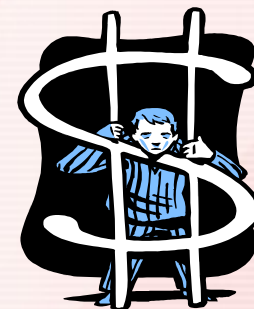
- Multiple or Unidentifiable Individuals Involved?
 - Provide generalized notice to the potentially affected population.
- Can't Notify the Individual Within 10 Days?
 - Notify the Deputy Secretary of Defense and the Defense Privacy Office immediately.
 - Include reason for delay (e.g., notification delayed at request of law enforcement authorities).





Privacy Criminal Penalties

- What Privacy Violations May Lead to Criminal Penalties?
 - Collecting data w/o meeting the Federal Register publication requirement.
 - Sharing data with unauthorized individuals.
 - Acting under false pretenses.
 - Facilitating those acting under false pretenses.
- Penalties:
 - Misdemeanor Charge (jail time of up to one year).
 - Fines of up to \$5,000 (for each offense).





Privacy Civil Penalties

- What Privacy Violations May Lead to Civil Penalties?
 - Unlawfully refusing to amend a record or grant access.
 - Failure to maintain accurate, relevant, timely, and complete data.
 - Failure to comply with any Privacy Act provision or agency rule that results in any adverse effect.
- Penalties:
 - Actual Damages
 - Attorney Fees
 - Removal from Employment





“Code of Fair Information Principles”

In order to assure that any personal information submitted to DLA is properly protected, DLA has devised a list of principles to be applied when handling personal information. This is referred to as the “**Code of Fair Information Principles.**”

The **Code** is set forth in a list of 10 policies that the DLA workforce will follow when handling personal information. Any DLA civilian, military member, or contractor employee who handles the personal information of others must abide by the principles set forth by the **Code.**



“Code of Fair Information Principles” (cont’d)

- 1. The Principle of Openness:** When we collect personal data from you, we will inform you of the intended uses of the data, the disclosures that will be made, the authorities for the collection, and whether the collection is mandatory or voluntary. We will collect no data subject to the Privacy Act unless a Privacy Act system notice has been published in the Federal Register.
- 2. The Principle of Individual Participation:** Unless an exemption has been claimed from the Privacy Act, we will, upon request, grant you access to your records; provide you a list of disclosures made outside the DoD; and make corrections to your file, once shown to be in error.
- 3. The Principle of Limited Collection:** DLA will collect only those personal data elements required to fulfill an official function or mission grounded in law. Those collections are conducted by lawful and fair means.



“Code of Fair Information Principles” (cont’d)

- 4. The Principle of Limited Retention:** DLA will retain your personal information only as long as necessary to fulfill the purposes for which it is collected, and then destroy it.
- 5. The Principle of Data Quality:** DLA strives to maintain only accurate, relevant, timely, and complete data about you.
- 6. The Principle of Limited Internal Use:** DLA will use your personal data only for lawful purposes, and limit access to those individuals with an official need for access.
- 7. The Principle of Disclosure:** The DLA workforce will zealously guard your personal data to ensure that all disclosures are made with your written permission or are made in strict accordance with the Privacy Act.



“Code of Fair Information Principles” (cont’d)

8. The Principle of Security: Your personal data is protected by appropriate physical, administrative, and technical safeguards to ensure security and confidentiality.

9. The Principle of Accountability: DLA and its workforce (civilian, military, and contractors) are subject to civil and criminal penalties for certain breaches of Privacy. DLA is diligent in sanctioning individuals who violate the Privacy Act.

10. The Principle of Challenging Compliance: You may challenge DLA if you believe that DLA has failed to comply with these principles, the Privacy Act, or the system of records notice.



SIDEBAR: Supervisor's Notes Are they personal or agency records?

Supervisor's notes are sometimes requested under the Freedom of Information Act (FOIA). "Personal" records of employees are excluded from FOIA coverage. Below are some questions that are examined when determining whether supervisor's notes would be considered an "agency" record or a "personal" record:

- Were they created on government time?
- Were they shared with other employees/officials?
- Were they filed with official agency records?
- Were they used in the decisionmaking process?
- Were they required to be created by rule, policy, or custom?

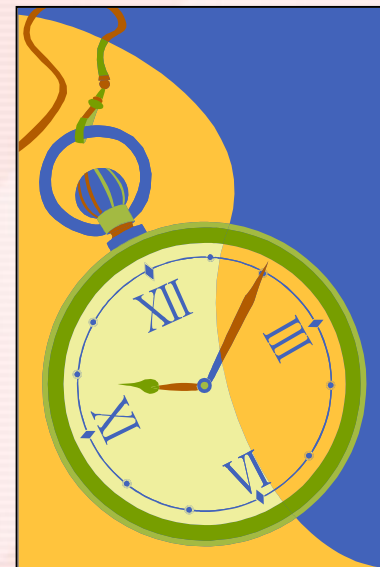




Sidebar: Supervisor's Notes

Were notes created on Government time?

- “Agency records” are generally those documents that are created or received in the course of conducting agency business. Despite that definition, not all files created on Government time are automatically regarded as “agency” records.
- The reverse is also true. Records you create on your personal time may rise to “agency” records - depending on how they are used and filed within DLA.
- So the use of government time is not always 100% determinative. Thus, the timing of creation must be examined in conjunction with the others factors.





Sidebar: Supervisor's Notes Were the notes shared with other employees?

- Once you share your notes with Human Resources, Counsel, or other third parties, they generally lose their “personal” status.
- Keeping your notes close-hold until the time is ripe to share them protects employee privacy and allows you to make fair decisions unencumbered by special interest concerns.





Sidebar: Supervisor's Notes

Were notes filed with official agency records?

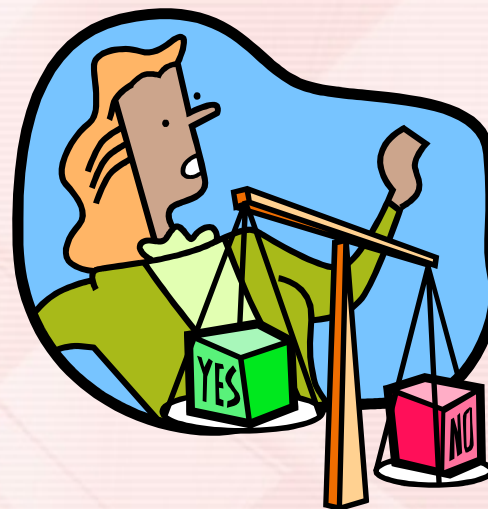
- Once notes are filed with official agency records, they lose their “personal record” status.
- Filing them separately, such as in a locked desk drawer or your briefcase, helps protect their “personal” status.





Sidebar: Supervisor's Notes Were they used in the decisionmaking process?

- Generally, once supervisors use their notes in deciding employee appraisals, taking disciplinary actions, rewarding exceptional workers, or similar uses, the notes become “agency” records.
- In adverse action situations, the notes may be required to be disclosed to the employee as part of the disciplinary process.





Sidebar: Supervisor's Notes Were they required to be created by rule, policy, or custom?

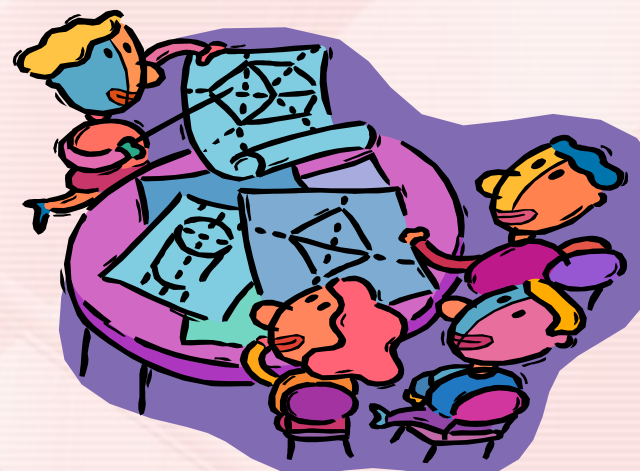
- In some cases, the taking of notes is required to be accomplished by rule, policy, or custom. In those cases, the notes would be deemed to be “agency” records.
- Examples:
 - Notes taken by a recording secretary during a meeting.
 - Notes taken by an individual assigned to route incoming emergency telephone calls.
 - Notes taken by an individual assigned to receive Defense “Hotline” telephone calls.

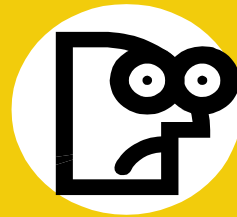
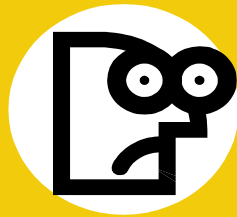




Conclusions

You and your staff are entrusted with the personal information of others. You are the first line of defense in safeguarding privacy and protecting DLA from damaging lawsuits.





It's QUESTION TIME !!



9 Questions to Test your Knowledge!

(Answers appear on the slide immediately following)

Q1: Which of the following is not a goal of the Privacy Act?

- a. Keeping personal information out of the hands of government.
- b. Eliminating "secret" file systems by letting the public know about data collections.
- c. Establishing and guaranteeing rights of data subjects.
- d. Establishing rules for collecting, using, and safeguarding data.



Answer

Q1: Which of the following is not a goal of the Privacy Act?

- a. Keeping personal information out of the hands of government.**
- b. Eliminating "secret" file systems by letting the public know about data collections.
- c. Establishing and guaranteeing rights of data subjects.
- d. Establishing rules for collecting, using, and safeguarding data.

See Slides 2, 3, and 4 for more information



Question

Q2: The Privacy Act protects:

- a. Only U.S. citizens and lawfully admitted aliens.
- b. Federal, state, and local government workers only.
- c. All individuals and business entities.
- d. All of the above.



Answer

Q2: The Privacy Act protects:

- a. Only U.S. citizens and lawfully admitted aliens.**
- b. Federal, state, and local government workers only.
- c. All individuals and business entities.
- d. All of the above.

See Slide 3 for more information



Question

Q3: The Privacy Act covers data held in "systems of records." A "system" consists of –

- a. Any group of files maintained electronically.
- b. A group of files containing Social Security Numbers.
- c. A group of files that are retrieved by personal identifier and contain, in addition to identifier, one other element of personal data about the individual.
- d. None of the above.



Answer

Q3: The Privacy Act covers data held in "systems of records." A "system" consists of –

- a. Any group of files maintained electronically.
- b. A group of files containing Social Security Numbers.
- c. A group of files that are retrieved by personal identifier and contain, in addition to identifier, one other element of personal data about the individual.**
- d. None of the above.

See Slide 3 for more information



Question

Q4: Who must comply with the Privacy Act?

- a. All U.S. citizens.
- b. All Executive Branch Federal employees, military members, and Federal contractors.
- c. Only supervisors of persons who collect or maintain personal information in a system of records.
- d. Only those persons who collect and use data.



Answer

Q4: Who must comply with the Privacy Act?

- a. All U.S. citizens.
- b. All Executive Branch Federal employees, military members, and Federal contractors.**
- c. Only supervisors of persons who collect or maintain personal information in a system of records.
- d. Only those persons who collect and use data.

See Slide 2, 5, and 6 for more information



Question

Q5: Which of the following would be inappropriate to discuss at your next staff meeting?

- a. The upcoming week's work schedule.
- b. Your serious commitment to Privacy Act principles and your expectations of staff.
- c. The good work of one employee in meeting a short deadline.
- d. The fact that you are considering disciplinary action against an employee based on notes you've been keeping.



Answer

Q5: Which of the following would be inappropriate to discuss at your next staff meeting?

- a. The upcoming week's work schedule.
- b. Your serious commitment to Privacy Act principles and your expectations of staff.
- c. The good work of one employee in meeting a short deadline.

d. The fact that you are considering disciplinary action against an employee based on notes you've been keeping.

“d” for two reasons: (1) Prematurely discussing details in your notes could cause them to lose their "personal record" status, and (2) Any discussion with staff should not occur until after the action is approved. Even then, details should be limited to those core facts the staff needs to know.

See Slides 12, 24, and 28.



Question

Q6: The penalties for violating the Privacy Act include which of the following?

- a. Jail time of up to one year.
- b. Fines of up to \$5,000.
- c. Removal from employment.
- d. All of the above



Answer

Q6: The penalties for violating the Privacy Act include which of the following?

- a. Jail time of up to one year.
- b. Fines of up to \$5,000.
- c. Removal from employment.

d. All of the above

See Slides 20 and 21 for more information.



Question

Q7: Which of the following statements are true?

- a. Supervisors have a duty to ensure their staff members comply with the Privacy Act.
- b. Supervisors may waive Privacy requirements during peak periods of heavy work provided the waiver is in writing.
- c. Supervisors must ensure their staff members have received Privacy training.
- d. Supervisors may recommend disciplinary action for a staff member who fails to follow Privacy rules.
- e. All are true.



Answer

Q7: Which of the following statements are true?

- a. Supervisors have a duty to ensure their staff members comply with the Privacy Act.**
- b. Supervisors may waive Privacy requirements during peak periods of heavy work provided the waiver is in writing.
- c. Supervisors must ensure their staff members have received Privacy training.**
- d. Supervisors may recommend disciplinary action for a staff member who fails to follow Privacy rules.**
- e. All are true.

No individual has authority to waive Privacy Act compliance.

See Slides 6, 7, and 25 for more information.



Question

Q8: Supervisors need not be concerned with the safeguarding of electronic records since that is controlled by the Information Technology staff.

TRUE or FALSE?



Answer

Q8: Supervisors need not be concerned with the safeguarding of electronic records since that is controlled by the Information Technology staff.

TRUE or **FALSE?**

While the IT staff establishes technical protocols to protect data, supervisors have a duty to ensure that staff members are following those protocols and that breaches are reported.

See Slides 6, 9 and 11-13 for more information.



Question

Q9: Which of the following statements are true regarding the use of shared calendars?

- a. It is OK to show that an employee is on sick leave.
- b. It is OK to show that an employee is teleworking.
- c. It is OK to show that an employee is away at a professional meeting.
- d. It is OK to show that an employee is on a compressed day off.
- e. It is OK to show that an employee is on LWOP.
- f. It is OK to show that an employee is on leave.



Answer

Q9: Which of the following statements are true regarding the use of shared calendars?

a. It is OK to show that an employee is on sick leave.

b. It is OK to show that an employee is teleworking.

c. It is OK to show that an employee is away at a professional meeting.

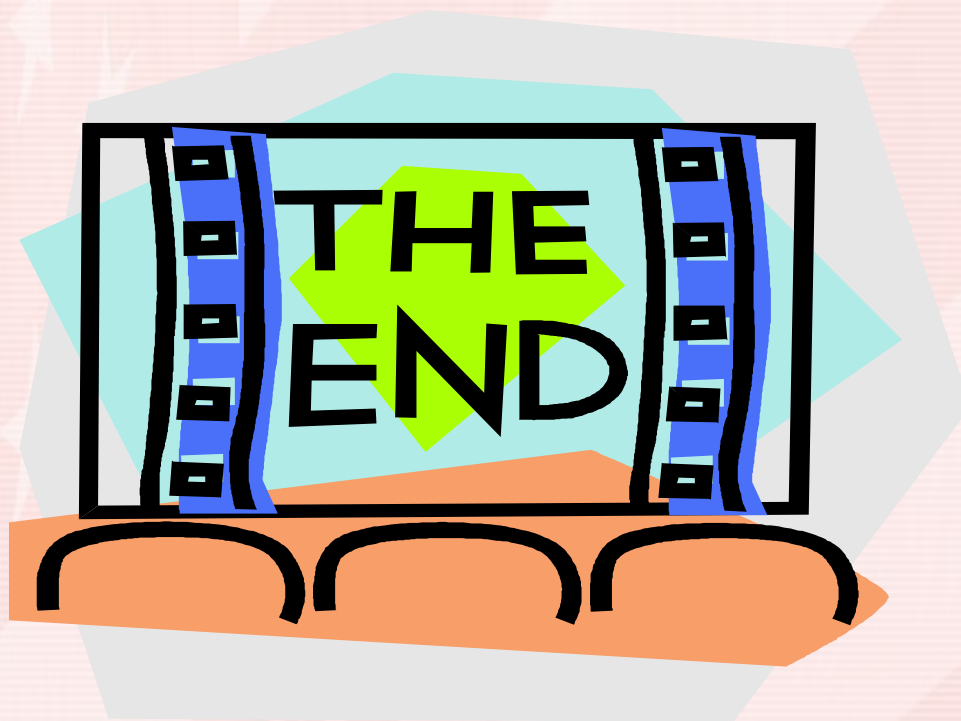
d. It is OK to show that an employee is on a compressed day off.

e. It is OK to show that an employee is on LWOP.

f. It is OK to show that an employee is on leave.

The use of sick, annual, family, religious, LWOP or AWOL should never be entered on shared calendars.

See Slides 12 and 16 for more information.





For More Information, Contact:



**Jody Sinkler
DLQ HQ Privacy Act Officer
Defense Logistics Agency
703-767-5045**

jody.sinkler@dla.mil

Or

**Lew Oleinick
DLA Privacy Technical Advisor
Defense Logistics Agency
703-767-6194**

lewis.oleinick@dla.mil



Certificate of Completion

Congratulation on the completion of
Privacy Act 102
Privacy Training for
DLA Supervisors / Managers